

**Notice of Allowability**

Application No.

10/789,373

Examiner

April Y. Shan

Applicant(s)

SEIFERT ET AL.

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith, (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/18/2004.
2. ☒ The allowed claim(s) is/are 1, 4 and 6-8.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some\* c) ☐ None of the:
- ☒ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
- \* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Notice of Informal Patent Application                      |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____. |
| 3. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date <u>2/27/2004</u> | 7. <input type="checkbox"/> Examiner's Amendment/Comment                               |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material                    | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance   |
|   | 9. <input type="checkbox"/> Other _____.   |

### **DETAILED ACTION**

1. This action is in response to the preliminary amendment filed 8/18/2004. Claims 1, 4 and 6-8 have been amended. Claims 2-3, 5 and 9 have been cancelled.

#### ***Allowable Subject Matter***

2. Claims 1, 4 and 6-8 are allowed.

### **REASONS FOR ALLOWANCE**

3. The following is an examiner's statement of reasons for allowance: The present invention is directed to a device/method for improving the safety of the RSA Chinese Residue Theorem (CRT) calculations against cryptographic attacks, a randomization of the auxiliary exponents and/or a change of the sub-moduli are performed. Independent claims 1 and 8 address a device/method for calculating a result of a modular exponentiation within an asymmetrical cryptosystem,  $n$  being a modulus,  $d$  being an exponent and a private key of the asymmetrical cryptosystem,  $c$  being a quantity to be subjected to the modular exponentiation, and as a result, a quantity  $m$  is obtained which equals the modular exponentiation of  $c$  with the private key  $d$  as an exponent, comprising means for/steps of calculating eight auxiliary quantities and means for/steps for calculating the results of the modular exponentiation  $m$  in case no error has been indicated. These features are neither shown or fairly suggested in the prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

Art Unit: 2135

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).


***Contact Information***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS  
9 March 2007  
AYS

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100